STATE OF ALABAMA

Information Technology Standard

Standard 600-04S1_Rev A: Incident Response Controls

1. INTRODUCTION:

An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. This State Standard provides the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

2. OBJECTIVE:

Ensure State agencies are prepared to respond to cyber security incidents, to protect State systems and data, and prevent disruption of government services.

3. SCOPE:

These requirements apply to all State of Alabama information system owners, agency information security officers, and other personnel (including employees, contractors, vendors, and business partners) responsible for developing cyber security incident response procedures.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: Recommended Security Controls for Federal Information Systems, State of Alabama cyber security incident response programs shall implement the following controls:

4.1 INCIDENT RESPONSE CONTROLS FOR ALL SYSTEMS

The following controls are applicable to all State of Alabama information systems:

4.1.1 Incident Response Policy and Procedures

Organizations that support information systems shall develop, disseminate, and periodically review/update:

(i) a formal, documented, incident response policy that addresses purpose/objective, scope, roles and responsibilities, and compliance/enforcement (State IT Policy 600-04 and this Standard satisfy this requirement); and

(ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Incident response procedures shall be developed for the security program in general and as required for particular information systems.

4.1.2 Incident Handling

Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Incorporate the lessons learned from prior and ongoing incident handling activities into the applicable incident response procedures.

4.1.3 Incident Reporting

Promptly report cyber security incident information to appropriate authorities in accordance with State or organization incident reporting procedures.

Ensure the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, directives, policies, regulations, standards, and procedures.

4.1.4 Incident Response Assistance

Organizations that support information systems shall provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. This support resource shall be an integral part of the organization's incident response capability.

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

4.2 ADDITIONAL CONTROLS FOR MODERATE AND HIGH IMPACT SYSTEMS

Organizations supporting incident response capabilities for moderate and high impact systems (see Definitions) shall further enhance all of the above control requirements by employing automated mechanisms where possible.

The following additional controls shall also be applied to moderate and high-impact systems:

4.2.1 Incident Response Training

Organizations shall train personnel in their incident response roles and responsibilities with respect to the information systems they support. Provide annual refresher training.

4.2.2 Incident Response Testing

Organizations shall test the incident response capability for the information systems they support at least annually using organization-defined tests, simulated events, and exercises to determine the incident response effectiveness. Document the results.

4.2.3 Incident Monitoring

Organizations shall track and document information system security incidents on an ongoing basis. Possible implementations of ongoing monitoring include automated monitoring and alerting systems, automatic notifications, and incident metrics.

5. DEFINITIONS:

HIGH-IMPACT SYSTEM: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high.

The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

(ii) result in major damage to organizational assets;

(iii) result in major financial loss; or

(iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

MODERATE-IMPACT SYSTEM: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.

The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

Serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

(ii) result in significant damage to organizational assets;

(iii) result in significant financial loss; or

(iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 600-04: Cyber Security Incident Response

6.2 RELATED DOCUMENTS

Information Technology Procedure 600-04P1: Incident Reporting

Information Technology Procedure 600-04P2: Incident Handling

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	1/12/2007	
Rev A	4/16/2008	Extended section 4.2 controls to apply to both moderate and high-impact systems; modified scope and definitions; added definition for moderate-impact systems.